ON THE INVARIANTS OF MATRICES AND THE EMBEDDING PROBLEM

F. Vaccarino

Abstract

Let $\mathbb{K}$ be an infinite field and let R be a $\mathbb{K}$-algebra endowed with a homogeneous polynomial norm N of degree n. We will show that R is a quotient of a ring of invariants of $n \times n$ matrices, if N satisfies a formal analogue of the Cayley-Hamilton Theorem. To achieve this we use recent results on invariants of matrices in positive characteristic, due to S. Donkin and A. Zubkov. This is a first step towards proving a characteristic-free generalization of the main theorem proved in [8], which gives sufficient conditions for an algebra over a characteristic zero field to be embeddable into a ring of matrices of order n over a commutative ring.

Introduction

Let $\mathbb{K}$ be an infinite field and let R be a $\mathbb{K}$-algebra, we would like to find sufficient conditions for the existence of a commutative $\mathbb{K}$-algebra, say L, such that R is embeddable into $M_n(L)$, the ring of $n \times n$ matrices over L.

It is known (see [7], [8], [9]) that, given any ring R there exist a unique commutative ring $A_n(R)$ and a unique ring homomorphism $j_n^R : R \longrightarrow M_n(A_n(R))$ such that, for any commutative ring B, $\mathrm{Hom}(R, M_n(B))$ is in bijection with $\mathrm{Hom}(A_n(R), B)$ via j_n^R. We will recall the construction of $(A_n(R), j_n^R)$ in the third section.

It is clear that R can be embedded into a ring of $n \times n$ matrices over a commutative ring if and only if j_n^R is a monomorphism.

The following result is proved in [8] .

Typeset by $\mathcal{AMS}$-TEX

Theorem (C. Procesi). *If R is a $\mathbb{Q}$-algebra with trace satisfying the n-th Cayley-Hamilton identity and $j_n^R : R \longrightarrow M_n(A_n(R))$ is the universal map we have that*

$$j_n^R : R \longrightarrow M_n(A_n(R))^{GL_n(\mathbb{Q})}$$

is an isomorphism.

The proof goes as follows: first, any $\mathbb{Q}$-algebra R, with trace, satisfying the n-th Cayley-Hamilton identity is showed to be of the form D/J, where D is a ring of polynomial covariants of a suitable number of copies of the ring of $n \times n$ matrices over $\mathbb{Q}$ and J is closed under trace. Then the surjectivity of j_n^R follows easily from the linear reductivity of the general linear group over a characteristic zero field. The injectivity of the universal map is then proved by means of the Reynolds operator and using the stability of J under the trace.

Let R be a ring endowed with a homogeneous polynomial norm N of degree n. Let t be a variable commuting with the elements of R. Since N is polynomial we can define

$$\chi_r(t) := N(t - r),$$

for all $r \in R$.

If $\chi_r(r) = 0$, for all $r \in R$, we say that R is a *Cayley-Hamilton ring of degree n*.

By means of Newton's formulas it follows that any $\mathbb{Q}$-algebra with trace satisfying the n-th Cayley-Hamilton identity is a Cayley-Hamilton ring of degree n.

C. Procesi asked the author the following natural question.

Question (C. Procesi). *If R is a Cayley-Hamilton $\mathbb{K}$-algebra of degree n, is*

$$j_n^R : R \longrightarrow M_n(A_n(R))^{GL_n(\mathbb{K})}$$

an isomorphism?

The main result of this paper is to show that any Cayley-Hamilton $\mathbb{K}$-algebra of degree n is a quotient of the ring of polynomial covariants of a number of copies of $n \times n$ matrices over $\mathbb{K}$.

The paper is divided into three sections. In the first section we develop some generalities on polynomial laws and divided powers rings. In the second section we will prove the main result. In order to do this we link the theory of invariants of matrices to the one of polynomial mappings and polynomial identities. We use the Donkin-Zubkov Theorem on invariants of matrices in positive characteristic that gives a presentation of the ring of polynomial invariants of several matrices in positive characteristic.

In the last section a possible strategy for tackling the Question is outlined.

§0 Conventions and Notations

Except otherwise stated all the rings (algebras over a commutative ring) should be understood associative and with multiplicative identity.

We denote by $\mathbb{N}$ the set of non-negative integers and by $\mathbb{Z}$ the ring of integers.

Let R be a commutative ring and let n be any positive integer: we denote by $M_n(R)$ the ring of $n \times n$ matrices with entries in R.

Let A be a set, we denote by $\# A$ its cardinality.

For A a set and any additive monoid M, we denote by $M^{(A)}$ the set of functions $f : A \longrightarrow M$ with finite support.

Let $\alpha \in M^{(A)}$, we denote by $\mid \alpha \mid$ the (finite) sum $\sum_{a \in A} \alpha(a)$.

Let S be a set. We put

$F_S := \mathbb{Z}\langle x_s \rangle_{s \in S}$ for the free ring over S;

F_S^+ for the augmentation ideal of F_S (non-unital subring);

$\mathcal{M}_S^+$ for the free semigroup generated by $\{x_s\}_{s \in S}$.

Let $a \in \mathcal{M}_S^+$ then $d_s(a)$ denotes the degree of a in x_s, $\ell(a) := \sum_{s \in S} d_s(a)$ its length or total degree and $m(a) := (d_s(a))_{s \in S}$ its multidegree (once a well-ordering is fixed on S);

Let $a, b \in \mathcal{M}_S^+$, we set $a \equiv b$ if and only if a is obtained from b by a cyclic permutation of letters. This gives an equivalence relation on $\mathcal{M}_S^+$ and we denote by $\mathfrak{M}_S^+$ the set of its equivalence classes.

§1 Multiplicative Polynomial Laws

1.1 Let $\mathbb{K}$ be a commutative ring. Let us recall the definition of a kind of map between $\mathbb{K}$-modules that generalizes the concept of polynomial map between free $\mathbb{K}$-modules (see [10] or [12]).

Definition 1.1.1. Let A and B be two $\mathbb{K}$-modules. A *polynomial law* φ from A to B is a family of mappings $\varphi_{_L} : L \otimes_{\mathbb{K}} A \longrightarrow L \otimes_{\mathbb{K}} B$, with L varying in the family of commutative $\mathbb{K}$-algebras, such that the following diagram commutes:

$$\begin{array}{ccc} L \otimes_{\mathbb{K}} A & \xrightarrow{\varphi_{_L}} & L \otimes_{\mathbb{K}} B \\ {\scriptstyle f\otimes 1_{_A}}\big\downarrow & & \big\downarrow{\scriptstyle f\otimes 1_{_B}} \\ M \otimes_{\mathbb{K}} A & \xrightarrow{\varphi_{_M}} & M \otimes_{\mathbb{K}} B, \end{array}$$

for all L, M commutative $\mathbb{K}$-algebras and all homomorphisms of $\mathbb{K}$-algebras $f : L \longrightarrow M$.

Definition 1.1.2. Let $n \in \mathbb{N}$, if $\varphi_{_L}(au) = a^n \varphi_{_L}(u)$, for all $a \in L$, $u \in L \otimes_{\mathbb{K}} A$ and all commutative $\mathbb{K}$-algebras L, then φ will be said *homogeneous of degree n*.

Definition 1.1.3. If A and B are two $\mathbb{K}$-algebras and

$$\begin{cases} \varphi_{_L}(xy) & = \varphi_{_L}(x)\varphi_{_L}(y) \\ \varphi_{_L}(1_{_{L\otimes A}}) & = 1_{_{L\otimes B}}, \end{cases}$$

for all commutative $\mathbb{K}$-algebras L and for all $x, y \in L \otimes A$, then φ is called *multiplicative*.

Let A and B be two $\mathbb{K}$-modules and $\varphi : A \to B$ be a polynomial law. We recall the following result on polynomial laws, which is a restatement of Théorème I.1 of [10].

Proposition 1.1.4. *Let S be a set.*

(1) *Let $L = \mathbb{K} \otimes F_S$ and let $\{a_s : s \in S\} \subset A$ be such that $a_s = 0$ except for a finite number of $s \in S$, then there exist $\varphi_\xi((a_s)) \in B$, with $\xi \in \mathbb{N}^{(S)}$, such that:*

$$\varphi_{_L}(\sum_{s\in S} x_s \otimes a_s) = \sum_{\xi \in \mathbb{N}^{(S)}} x^\xi \otimes \varphi_\xi((a_s)),$$

where $x^\xi := \prod_{s\in S} x_s^{\xi_s}$.

(2) *Let* R *be any commutative* $\mathbb{K}$*-algebra and let* $(r_s)_{s\in S} \subset R$*, then:*

$$\varphi_R(\sum_{s\in S} r_s \otimes a_s) = \sum_{\xi\in\mathbb{N}^{(S)}} r^\xi \otimes \varphi_\xi((a_s)),$$

where $r^\xi := \prod_{s\in S} r_s^{\xi_s}$.

(3) *If* φ *is homogeneous of degree* n*, then in the previous sum one has* $\varphi_\xi((a_s)) = 0$ *if* $\mid \xi \mid$ *is different from* n*. That is:*

$$\varphi_R(\sum_{a\in A} r_a \otimes a) = \sum_{\xi\in\mathbb{N}^{(A)},\, |\xi|=n} r^\xi \otimes \varphi_\xi((a)).$$

In particular, if φ *is homogeneous of degree* 0 *or* 1*, then it is constant or linear, respectively.*

Let S be a set, Proposition 1.1.4 means that a polynomial law $\varphi : A \longrightarrow B$ is completely determined by its coefficients $\varphi_\xi((a_s))$, with $(a_s)_{s\in S} \in A^{(S)}$.

Remark 1.1.5. If A is a free $\mathbb{K}$-module and $\{a_t : t \in T\}$ is a basis of A, then φ is completely determined by its coefficients $\varphi_\xi((a_t))$, with $\xi \in \mathbb{N}^{(T)}$. If also B is a free $\mathbb{K}$-module with basis $\{b_u : u \in U\}$, then $\varphi_\xi((a_t)) = \sum_{u\in U} \lambda_u(\xi) b_u$. Let $a = \sum_{t\in T} \mu_t a_t \in A$. Since only a finite number of μ_t and $\lambda_u(\xi)$ are different from zero, the following makes sense:

$$\varphi(a) = \varphi(\sum_{t\in T} \mu_t a_t) = \sum_{\xi\in\mathbb{N}^{(T)}} \mu^\xi \varphi_\xi((a_t)) = \sum_{\xi\in\mathbb{N}^{(T)}} \mu^\xi(\sum_{u\in U} \lambda_u(\xi) b_u) = \sum_{u\in U}(\sum_{\xi\in\mathbb{N}^{(T)}} \lambda_u(\xi)\mu^\xi) b_u.$$

Hence, if both A and B are free $\mathbb{K}$-modules, a polynomial law between them is simply a polynomial map.

1.2 Let $\mathbb{K}$ be any commutative ring with identity. For a $\mathbb{K}$-module M let $\Gamma(M)$ denote its divided powers algebra (see [2], [10] and [12]). This is a unital commutative $\mathbb{K}$-algebra,

with generators $m^{(k)}$, with $m \in M$, $k \in \mathbb{Z}$ and relations, for all $m, n \in M$:

(i) $$m^{(i)} = 0, \qquad \forall i < 0;$$

(ii) $$m^{(0)} = 1_{\mathbb{K}}, \qquad \forall m \in M;$$

(iii) $$(rm)^{(i)} = r^i m^{(i)}, \qquad \forall r \in R, \forall i \in \mathbb{N};$$

(iv) $$(m+n)^{(k)} = \sum_{i+j=k} m^{(i)} n^{(j)}, \qquad \forall k \in \mathbb{N};$$

(v) $$m^{(i)} m^{(j)} = \binom{i+j}{i} m^{(i+j)}, \qquad \forall i, j \in \mathbb{N}.$$

The $\mathbb{K}$-module $\Gamma(M)$ is generated by products (over arbitrary index sets I) $\prod_{i\in I} x_i^{(\alpha_i)}$ of the above generators, it is clear that $\prod_{i\in I} x_i^{(\alpha_i)} = 0$ if $\alpha_i < 0$ for some $i \in I$. The divided powers algebra $\Gamma(M)$ is a $\mathbb{N}$-graded algebra with homogeneous components $\Gamma_k := \Gamma_k(M)$, ($k \in \mathbb{N}$), the submodule generated by $\{\prod_{i\in I} x_i^{(\alpha_i)} \ : \ |\alpha| = k\}$. Note that $\Gamma_0 \cong \mathbb{K}$ and $\Gamma_1 \cong M$. Γ is a functor from $\mathbb{K}$-modules to commutative unital graded $\mathbb{K}$-algebras.

Indeed for any morphism of $\mathbb{K}$-modules $f : M \longrightarrow N$ there exists a unique morphism of graded $\mathbb{K}$-algebras $\Gamma(f) : \Gamma(M) \longrightarrow \Gamma(N)$ such that $\Gamma(f)(x^{(n)}) = f(x)^{(n)}$, for any $x \in M$ and $n \geq 0$. From this it follows easily that Γ is exact.

Furthermore $\Gamma(L \otimes_{\mathbb{K}} M) \cong L \otimes_{\mathbb{K}} \Gamma(M)$ as graded rings by means of $(1 \otimes x)^{(n)} \mapsto 1 \otimes x^{(n)}$. Thus the map $\Gamma(f)$ commutes with extensions of scalars.

If A is a (unital) $\mathbb{K}$-algebra, then $\Gamma_k(A)$ is a (unital) $\mathbb{K}$-algebra too (see [11]). To distinguish the new multiplication on $\Gamma_k(A)$ from the one of $\Gamma(A)$, we denote it by "τ_k". We have:

$$\begin{aligned}\prod_{i\in I} a_i^{(\alpha_i)} \ \tau_k \ \prod_{j\in J} b_j^{(\beta_j)} &:= (\prod_{i\in I} a_i^{(\alpha_i)}) \ \tau_k \ (\prod_{j\in J} b_j^{(\beta_j)}) \\ &:= \sum_{(\lambda_{ij})\in M(\alpha,\beta)} \ \prod_{(i,j)\in I\times J} (a_i b_j)^{(\lambda_{ij})},\end{aligned}$$

where $M(\alpha, \beta) := \{(\lambda_{ij}) \in \mathbb{N}^{(I\times J)} : \sum_{i\in I} \lambda_{ij} = \beta_j \ , \forall j \in J \ ; \sum_{j\in J} \lambda_{ij} = \alpha_i \ , \forall i \in I\}$ and $\prod_{i\in I} a_i^{(\alpha_i)}, \prod_{j\in J} b_j^{(\beta_j)} \in \Gamma_k(A)$.

Let us denote by $\gamma_n := (\gamma_{n,L})$ the polynomial law given by the composition $L \otimes M \longrightarrow \Gamma_n(L \otimes M) \longrightarrow L \otimes \Gamma_n(M)$, then γ_n is homogeneous of degree n.

There is a property proved by Roby in [11], which motivates our introduction of divided powers.

Theorem 1.2.1. *Let A and B be two $\mathbb{K}$ -algebras. The set of homogeneous multiplicative polynomial laws of degree n from A to B is in bijection with the set of all homomorphisms of $\mathbb{K}$-algebras from $\Gamma_n(A)$ to B. Namely, given any homogeneous multiplicative polynomial law $f : A \longrightarrow B$ of degree n, there exists a unique homomorphism of $\mathbb{K}$-algebras $\phi : \Gamma_n(A) \longrightarrow B$ such that $f_L = (1_L \otimes \phi) \cdot \gamma_{n,L}$, for any commutative $\mathbb{K}$-algebra L.*

1.3 Let B be a commutative ring and let $M_n(B)$ be the ring of $n \times n$ matrices over B. Let $b \in M_n(B)$ and denote by $e_i(b)$ the i-th coefficient of the characteristic polynomial of b, i.e. the trace (up to sign) of $\wedge^i(b)$.

Let R be a ring, we denote by $(R)^{ab}$ its abelianization, that is, its quotient by the ideal generated by the commutators of its elements.

The following can be found in [13].

Proposition 1.3.1. *The ring $\Gamma_n(M_n(B))^{ab}$ is isomorphic to B. The canonical projection $\mathfrak{ab}_n := \Gamma_n(M_n(B)) \longrightarrow \Gamma_n(M_n(B))^{ab}$ is such that, for all $b \in M_n(B)$ and $0 \leq i \leq n$,*

$$\mathfrak{ab}_n(1^{(n-i)} b^{(i)}) = e_i(b).$$

1.4 Let M be a free $\mathbb{K}$-module and let $\{m_i \,:\, i \in I\}$ be a $\mathbb{K}$-basis of M, I a set. Then $\Gamma_n(M)$ is a free $\mathbb{K}$-module and $\{\prod_{i \in i} m_i^{(\alpha_i)} \,:\, \alpha \in \mathbb{N}^{(I)}$ with $\mid \alpha \mid= n\}$ is a $\mathbb{K}$-basis of it. Now, F_S is a free $\mathbb{Z}$-module with basis $\{1\} \cup \mathcal{M}_S^+$, thus

$$\mathcal{B}_n := \{1^{(n-|\alpha|)} \prod_{\mu \in \mathcal{M}_S^+} \mu^{(\alpha_\mu)} \,:\, \alpha \in \mathbb{N}^{(\mathcal{M}_S^+)} \text{ with } \mid \alpha \mid \leq n\}$$

is a $\mathbb{Z}$-basis of $\Gamma_n(F_S)$ and we will refer to this as the *standard basis*.

Another remark is that the natural multidegree of F_S induce another on $\Gamma_n(F_S)$ defining $m(1^{(n-|\alpha|)} \prod_{\mu \in \mathcal{M}_S^+} \mu^{(\alpha_\mu)}) := \sum_{\mu \in \mathcal{M}_S^+} \alpha_\mu m(\mu)$ (see §0). The product defined above makes then $\Gamma_n(F_S)$ into a graded ring, with respect to this multidegree, as can be easily cheked.

For further readings on these topics we refer to [2], [10], [11], [12] and [13].

§2 Divided Powers and Invariants of Matrices

2.1 Let us introduce the following notation: let S be a set, we put

$A_S(n) := \mathbb{Z}[x^s_{ij}]_{1\leq i,j\leq n\,,\,s\in S}$, the symmetric algebra on the direct sum of $\#S$ copies of $M_n(\mathbb{Z})$;

$B_S(n) := M_n(A_S(n))$;

$G := Gl_n(\mathbb{Z})$;

$C_S(n) := A_S(n)^G$, the ring of invariants with respect to the action of G on $A_S(n)$ induced by simultaneous conjugation on the direct sum of $\#S$ copies of $M_n(\mathbb{Z})$;

2.2 Let $j_n : F_S \longrightarrow B_S(n)$ be given by

$$j_n(x_s) = \zeta_s := \sum_{i,j=1}^{n} x^s_{i,j} e_{i,j},$$

where $(e_{i,j})_{h,k} = \delta_{i,h}\delta_{j,k}$ for $i, j, h, k = 1, \ldots, n$. The ζ_s are the so-called "generic matrices of order n".

Let

$$\beta_n : \Gamma_n(B_S(n)) \longrightarrow \Gamma_n(B_S(n))^{ab}$$

be the canonical projection, then $A_S(n) \cong \Gamma_n(B_S(n))^{ab}$ by Prop.1.3.1.

We set

$$E_S(n) := \beta_n(\Gamma_n(j_n(F_S)) \hookrightarrow A_S(n),$$

by Prop.1.3.1 it is the subring of $A_S(n)$ generated by the $e_i(j_n(f))$, where $i \in \mathbb{N}$ and $f \in F_S$. By the exactness properties of Γ_n and $(-)^{ab}$ there exists a unique ring epimorphism

$$\pi_n : \Gamma_n(F_S)^{ab} \longrightarrow E_S(n)$$

such that the following diagram commutes:

$$\begin{array}{ccc} \Gamma_n(F_S) & \xrightarrow{\Gamma_n(j_n)} & \Gamma_n(j_n(F_S)) \\ \mathfrak{ab}_n \big\downarrow & & \big\downarrow \beta_n \\ \Gamma_n(F_S)^{ab} & \xrightarrow{\pi_n} & E_S(n). \end{array}$$

By Prop.1.3.1 it is clear that $\pi_n(1^{(n-i)}f^{(i)}) = e_i(j_n(f))$, for all $i \in \mathbb{N}$ and $f \in F_S$.

Remark 2.2.1. By the previous discussion the polynomial law $j_n(F_S) \longrightarrow E_S(n)$ that corresponds to β_n, via theorem 1.2.1, is the restriction to $j_n(F_S)$ of the determinant.

Recall that $E_S(n)$ is a subring of $C_S(n)$.

The Donkin-Zubkov Theorem on invariants of matrices can be stated in the following way, see [4], [5], [14] and [15]. (This Theorem was firstly proved by S. Donkin and then by A. Zubkov in another way).

Theorem (Donkin-Zubkov). *The ring $C_S(n)$ of polynomial invariants of the direct sum of $\#S$ copies of $n \times n$ matrices is equal to $E_S(n)$.*

Then we have a surjection $\pi_n : \Gamma_n(F_S)^{ab} \longrightarrow E_S(n) = C_S(n)$.

Let $\delta_n : A_S(n) \longrightarrow A_S(n-1)$ be the natural projection given by

$$x_{ij}^s \mapsto \begin{cases} 0 & \text{if } i = n \text{ or } j = n \\ x_{ij}^s & \text{otherwise.} \end{cases}$$

Notice that $(\delta_n)_{C_S(n)}\big(C_S(n)\big) = (\delta_n)_{E_S(n)}\big(E_S(n)\big) = E_S(n-1) = C_S(n-1)$ and denote again by δ_n its restriction to $C_S(n)$. We denote by C_S the inverse limit, in the category of graded rings, of the inverse system $\big(C_S(n), \delta_n\big)$.

In [15] the following is proved.

Theorem (Zubkov). *The following sequence is exact:*

$$0 \longrightarrow \langle \{e_{n+1+k}(f) \,:\, k \in \mathbb{N} \textit{ and } f \in F_S^+\} \rangle \longrightarrow C_S \xrightarrow{\theta_n} C_S(n) \longrightarrow 0,$$

where θ_n is the canonical projection from C_S to $C_S(n)$.

We are now able to state the main result of this section.

Theorem 2.2.2. *The map $\pi_n : \Gamma_n(F_S)^{ab} \longrightarrow C_S(n)$ is an isomorphism of graded rings.*

The proof of this splits into some lemmas.

Let us consider $\Gamma(F_S^+) = \oplus_{k\geq 0}\Gamma_k(F_S^+)$. It is a free $\mathbb{Z}$-module with basis

$$\mathcal{B} := \{ \prod_{\mu\in\mathcal{M}_S^+} \mu^{(\alpha_\mu)} \; : \; \alpha \in \mathbb{N}^{(\mathcal{M}_S^+)}\}.$$

So we can define a $\mathbb{Z}$-module epimorphism

$$\begin{aligned} \sigma_n : &\Gamma(F_S^+) \longrightarrow \Gamma_n(F_S) \\ &\prod_{\mu\in\mathcal{M}_S^+} \mu^{(\alpha_\mu)} \mapsto 1^{(n-|\alpha|)} \prod_{\mu\in\mathcal{M}_S^+} \mu^{(\alpha_\mu)} \end{aligned}$$

with $n \in \mathbb{N}$.

Lemma 2.2.3.

(1) *The kernel of σ_n is $\oplus_{h>n}\Gamma_h(F_S^+)$.*

(2) *There is a unique product τ on $\Gamma(F_S^+)$, that makes it an associative graded ring with identity $1 = \prod_{\mu\in\mathcal{M}_S^+} \mu^{(0)}$, multidegree given by*

$$m(\prod_{\mu\in\mathcal{M}_S^+} \mu^{(\alpha_\mu)}) := \sum_{\mu\in\mathcal{M}_S^+} \alpha_\mu m(\mu)$$

and such that σ_n is a graded ring homomorphism for all $n \in \mathbb{N}$, namely, for all $\prod_{\mu\in\mathcal{M}_S^+} \mu^{(\alpha_\mu)}, \prod_{\nu\in\mathcal{M}_S^+} \nu^{(\beta_\nu)} \in \mathcal{B}$:

$$(\prod_{\mu\in\mathcal{M}_S^+} \mu^{(\alpha_\mu)}) \,\tau\, (\prod_{\nu\in\mathcal{M}_S^+} \nu^{(\beta_\nu)}) := \sum_{\gamma\in\alpha\odot\beta} \prod_{\mu\in\mathcal{M}_S^+} \mu^{(\gamma_{\mu,1})} \prod_{\nu\in\mathcal{M}_S^+} \nu^{(\gamma_{1,\nu})} \prod_{(\mu,\nu)\in(\mathcal{M}_S^+)^2} \mu\nu^{(\gamma_{\mu,\nu})},$$

where $\alpha\odot\beta$ is the set of $(\gamma_{\mu,\nu}) \in \mathbb{N}^{(\mathcal{M}_S\times\mathcal{M}_S)}$ such that $\gamma_{1,1} = 0$ and

$$\begin{cases} \sum_{\nu\in\mathcal{M}_S} \gamma_{\mu,\nu} = \alpha_\mu, \; \text{for all } \mu \in \mathcal{M}_S^+ \\ \sum_{\mu\in\mathcal{M}_S} \gamma_{\mu,\nu} = \beta_\nu, \; \text{for all } \nu \in \mathcal{M}_S^+. \end{cases}$$

Proof.

(1) Follows from $\sigma_n\big(\oplus_{h>n}\Gamma_h(F_S^+)\big)=0$ and the fact that σ_n induces a bijection between

$$\{\prod_{\mu\in\mathcal{M}_S^+}\mu^{(\alpha_\mu)}\ :\ \alpha\in\mathbb{N}^{(\mathcal{M}_S^+)}\ \text{with}\ \mid\alpha\mid\leq n\}$$

and (see 1.4)

$$\{1^{(n-|\alpha|)}\prod_{\mu\in\mathcal{M}_S^+}\mu^{(\alpha_\mu)}\ :\ \alpha\in\mathbb{N}^{(\mathcal{M}_S^+)}\ \text{with}\ \mid\alpha\mid\leq n\}=\mathcal{B}_n.$$

(2) Let $\prod_{\mu\in\mathcal{M}_S^+}\mu^{(\alpha_\mu)}$, $\prod_{\nu\in\mathcal{M}_S^+}\nu^{(\beta_\nu)}\in\mathcal{B}$ and let

$$\tilde\alpha:=\big(n-|\alpha|,(\alpha_{mu})_{\mu\in\mathcal{M}_S^+}\big)\ \text{and}\ \tilde\beta:=\big(n-|\beta|,(\beta_\nu)_{\nu\in\mathcal{M}_S^+}\big),$$

then (see 1.2):

$$1^{(n-|\alpha|)}\prod_{\mu\in\mathcal{M}_S^+}\mu^{(\alpha_\mu)}\ \tau_n\ 1^{(n-|\beta|)}\prod_{\nu\in\mathcal{M}_S^+}\nu^{(\beta_\nu)}=\sum_{\gamma\in M(\tilde\alpha,\tilde\beta)}\ \prod_{(\mu,\nu)\in\mathcal{M}_S^2}(\mu\nu)^{(\gamma_{\mu,\nu})}. \tag{$*$}$$

Let $\gamma\in M(\tilde\alpha,\tilde\beta)$. By the definition of τ_n (see 1.2) one sees that:

$$\begin{cases}\sum_{\nu\in\mathcal{M}_S}\gamma_{\mu,\nu}=\alpha_\mu,\ \text{for all}\ \mu\in\mathcal{M}_S^+\\ \sum_{\mu\in\mathcal{M}_S}\gamma_{\mu,\nu}=\beta_\nu,\ \text{for all}\ \nu\in\mathcal{M}_S^+.\end{cases} \tag{$**$}$$

The result follows by writing the left hand side of $(*)$ as

$$\sum_{\gamma\in\alpha\odot\beta}1^{(n-|\gamma|)}\prod_{\mu\in\mathcal{M}_S^+}\mu^{(\gamma_{\mu,1})}\prod_{\nu\in\mathcal{M}_S^+}\nu^{(\gamma_{1,\nu})}\prod_{(\mu,\nu)\in(\mathcal{M}_S^+)^2}\mu\nu^{(\gamma_{\mu,\nu})}$$

where $\alpha\odot\beta$ is the set of $(\gamma_{\mu,\nu})\in\mathbb{N}^{(\mathcal{M}_S\times\mathcal{M}_S)}$ with $\gamma_{1,1}=0$ and satisfying $(**)$. $\square$

Let us denote by $\mathcal{P}_S$ the ring $(\Gamma(F_S^+),\tau)$.

Lemma 2.2.4.

(1) *The following is an epimorphism of graded rings for all $n\in\mathbb{N}$:*

$$\begin{aligned}\rho_n:&\Gamma_n(F_s)\longrightarrow\Gamma_{n-1}(F_s)\\ &1^{(n-|\alpha|)}\prod_{i\in I}a_i^{(\alpha_i)}\mapsto 1^{(n-1-|\alpha|)}\prod_{i\in I}a_i^{(\alpha_i)}.\end{aligned}$$

where $1^{(n-|\alpha|)}\prod_{i\in I} a_i^{(\alpha_i)} \in \Gamma_n(F_S)$.

(2) $\mathcal{P}_S$ *is the graded inverse limit of the inverse system* $\big(\Gamma_n(F_S),\rho_n\big)$ *and the* σ_n *are the canonical projections.*

(3) *The following is a commutative diagram in the category of graded rings for all* $n\in\mathbb{N}$*:*

$$\begin{array}{ccc}
\Gamma_n(F_S)^{ab} & \xrightarrow{(\rho_n)^{ab}} & \Gamma_{n-1}(F_S)^{ab} \\
{\scriptstyle\pi_n}\big\downarrow & & \big\downarrow{\scriptstyle\pi_{n-1}} \\
C_S(n) & \xrightarrow{\delta_n} & C_S(n-1).
\end{array}$$

(4) *There exists an epimorphism of graded rings* $\pi : \mathcal{P}_S^{ab} \longrightarrow C_S$ *such that* $\pi(f^{(i)}) = \varprojlim e_i(j_n(f))$ *for all* $f\in F_S^+$ *and* $i\in\mathbb{N}$.

Proof.

(1) It is a straightforward verification.

(2) By Lemma 2.2.3 (1) we have an decreasing filtration of ideals of $\mathcal{P}_S$:

$ker\sigma_n \subset ker\sigma_{n-1}$ and $\sigma_n(ker\sigma_{n-1}) = ker\rho_n$. Observe that $\{\big(1^{(n-|\alpha|)}\prod_{i\in I} a_i^{(\alpha_i)}\big)_{n\in\mathbb{N}} : \alpha\in\mathbb{N}^{(\mathcal{M}_S^+)}\}$ is a $\mathbb{Z}$-basis of the limit, and notice that $\big(1^{(n-|\alpha|)}\prod_{i\in I} a_i^{(\alpha_i)}\big)_{n\in\mathbb{N}} \mapsto \prod_{i\in I} a_i^{(\alpha_i)}$ is the required isomorphism.

(3) Let $I_n := \mathfrak{ab}_n\big(ker\rho_n\big)$, then $I_n = \langle\{\mathfrak{ab}_n(f^{(n)}) \,:\, f\in F_S^+\}\rangle$. Observe that $\pi_n\big(\mathfrak{ab}_n(f^{(n)})\big) = e_n(f)\in ker\delta_n$, for all $f\in F_S^+$.

(4) Follows directly from (3) applying the abelianization functor. $\square$

Let S_n be the symmetric group on n letters. It acts on the polynomial ring $\mathbb{Z}[x_1,x_2,\dots,x_n]$ by permuting the x_i's. This action preserve the degree and we denote by Λ_n^k the group of invariants of degree k, then $\Lambda_n := \mathbb{Z}[x_1,x_2,\dots,x_n]^{S_n} = \oplus_{k\geq 0}\Lambda_n^k$. Let $q_n : \mathbb{Z}[x_1,x_2,\dots,x_n] \longrightarrow \mathbb{Z}[x_1,x_2,\dots,x_{n-1}]$ be given by $x_n\mapsto 0$ and $x_i\mapsto x_i$, for $i=1,\dots,n-1$. This map sends Λ_n^k to Λ_{n-1}^k.Denote by Λ^k the limit of the inverse system obtained in this way. Define $\Lambda := \oplus_{k\geq 0}\Lambda^k$: this is the so-called ring of *symmetric functions*. Let $k\in\mathbb{N}$ and set

$$e_k(x_1,\dots,x_n) := \sum_{i_1<i_2<\dots<i_k} x_{i_1}x_{i_2}\cdots x_{i_k} \in \Lambda_n^k$$

to denote the k-th elementary symmetric polynomial in $x_1, x_2, \ldots, x_n$. It can be showed that the $e_k := \varprojlim e_k(x_1, x_2, \ldots, x_n)$ are such that $\Lambda = \mathbb{Z}[e_1, e_2, \ldots, e_k, \ldots]$.

In Λ we have a further operation beside the product: the *plethysm*. Let $g, f \in \Lambda$, we say that $h \in \Lambda$ is the plethysm of g by f and we denote it by $h = g \circ f$ if h is obtained by substituting the monomials appearing in f at the place of the variables in g. In Λ we have two other distinguished kind of functions beside the elementary symmetric: the *powers sums* and the *monomial symmetric functions*. For any $n \in \mathbb{N}$ the n-th power sum is $p_n := \sum_{i \geq 1} x_i^n$; for any $h \in \mathbb{N}$ and for any $\alpha = (\alpha_1, \ldots, \alpha_h) \in \mathbb{N}^h$, such that $\alpha_1 \geq \alpha_2 \geq \cdots \geq \alpha_h > 0$ the monomial symmetric function is $m_\alpha := \sum_f \prod_{i \geq 1}^h x_{f(i)}^{\alpha_i}$, where sum is taken over all the injections $f : \{1, \ldots, h\} \longrightarrow \mathbb{N}$. Let $g \in \Lambda$, then it is clear that $g \circ p_n = g(x_1^n, x_2^n, \ldots, x_k^n, \ldots)$.

Lemma 2.2.5.

(1) *The ring $\mathcal{P}_S$ is generated by the $\mu^{(i)}$ with $i \in \mathbb{N}$ and $\mu \in \mathcal{M}_S^+$.*

(2) *For all $a \in F_S^+$, and $n, i \in \mathbb{N}$, $(a^n)^{(i)}$ belongs to the subring of $\mathcal{P}_S$ generated by the $a^{(j)}$, for $0 \leq j \leq ni$. Furthermore $(a^n)^{(i)} = \rho_a(e_i \circ p_n)$, where $\rho_a : \Lambda \longrightarrow \mathcal{P}_S$ is the ring homomorphism defined by $e_j \mapsto a^{(j)}$.*

Proof.

(1) Observe that, for all $\alpha \in \mathbb{N}^k$, $a \in (\mathcal{M}_S^+)^k$ and $k \in \mathbb{N}$

$$a_1^{(\alpha_1)} a_2^{(\alpha_2)} \cdots a_k^{(\alpha_k)} = a_1^{(\alpha_1)} \tau\big(a_2^{(\alpha_2)} \cdots a_k^{(\alpha_k)}\big) - \sum a_1^{(\gamma_{1,0})} \prod_{j=2}^{k} a_j^{(\gamma_{0,j})} \prod_{j=2}^{k} a_1 a_j^{(\gamma_{1,j})},$$

where the sum is taken over all $\gamma \in (\alpha_1) \odot (\alpha_2, \ldots, \alpha_k)$ such that $\sum_{j=2}^k \gamma_{1,j} > 0$. Then

$$\sum_{i,j} \gamma_{ij} = \sum_i \alpha_i - \sum_{j=2}^{k} \gamma_{1,j} < \sum_i \alpha_i = |\alpha|.$$

Applying this reduction process inductively on $|\alpha|$, it is possible to express $a_1^{(\alpha_1)} a_2^{(\alpha_2)} \cdots a_k^{(\alpha_k)}$ as a polynomial in the $\mu^{(i)}$, with $i \in \mathbb{N}$ and μ a monomial in the a_j.

(2) Let $a \in F_S^+$ and let t be a variable commuting with the x_s. Let us set

$$\varphi(1+ta) := \sum_{j\geq 0} t^j a^{(j)},$$

then φ is a polynomial law $\mathbb{Z}[t] \otimes_{\mathbb{Z}} F_S^+ \longrightarrow \mathbb{Z}[[t]] \otimes \mathcal{P}_S$ which is multiplicative as can be easily checked.

Let ϵ be a primitive n-th root of unity. Since $1 - t^n a^n = \prod_{k=1}^n (1-\epsilon^k ta)$, we have

$$\begin{aligned}\sum_{j\geq 0}(-1)^j t^{nj}(a^n)^{(j)} = \varphi(1-t^n a^n) = \prod_{k=1}^{n} \varphi(1-\epsilon^k ta) = \\ = \prod_{k=1}^{n} \Big(\sum_{j_k \geq 0} (-1)^{j_k} t^{j_k} a^{(j_k)} \Big) = \sum_{h\geq 0} (-1)^h t^h \sum_{j_1+\cdots+j_n=h} \prod_{k=1}^{n} a^{(j_k)} \epsilon^{j_1+2j_2+\cdots+nj_n} \\ = \sum_{h\geq 0}(-1)^h t^h \sum_{\alpha\in P_{h,n}} \Big(\prod_{k=1}^{n} a^{(\alpha_k)}\Big)\, m_\alpha(\epsilon,\ldots,\epsilon^{n-1},1),\end{aligned}$$

where $P_{h,n}$ denotes the set of partitions of h in at most n parts and $m_\alpha(x_1,\ldots,x_n)$ is the monomial symmetric polynomial associated to α.

The elementary symmetric polynomial $e_i \in \Lambda_n$ satisfy

$$e_i(\epsilon,\ldots,\epsilon^{n-1},1) = \begin{cases} 0 & 1 \leq i \leq n-1 \\ 1 & i = n. \end{cases}$$

thus

$$m_\alpha(\epsilon,\ldots,\epsilon^{n-1},1) = \begin{cases} 0 & n \nmid |\alpha| \\ c_\alpha \in \mathbb{Z} & \text{otherwise,} \end{cases}$$

where c_α is the coefficient of the $(|\alpha|/n)$-th power of e_n that appears in the expansion of m_α on $e_1,\ldots,e_n$ in Λ_n. Therefore

$$\sum_{j\geq 0}(-1)^j t^{nj}(a^n)^{(j)} = \sum_{j\geq 0}(-1)^{nj} t^{nj} \sum_{\alpha\in P_{nj,n}} \Big(\prod_{k=1}^{n} a^{(\alpha_k)}\Big)\, c_\alpha,$$

thus

$$(a^n)^{(i)} = (-1)^{(n+1)i} \sum_{\alpha\in P_{ni,n}} \Big(\prod_{k=1}^{n} a^{(\alpha_k)}\Big)\, c_\alpha.$$

The assertion follows since this last equality is the image by ρ_a of the one defining the plethysm $e_i \circ p_n$. $\square$

A monomial in $\mathcal{M}_S^+$ is called *indecomposable* if it is not a power of another. Let $\psi \subset \mathfrak{M}_S^+$ be the set of (equivalence classes with respect to cyclic permutations of) indecomposable monomials. Let $\mathfrak{ab} : \mathcal{P}_S \longrightarrow \mathcal{P}_S^{ab}$ be the canonical projection.

Lemma 2.2.6. *The map $\pi : \mathcal{P}_S^{ab} \longrightarrow C_S$ is an isomorphism.*

Proof. It is easy to see, by induction on $i \in \mathbb{N}$ that $\mathfrak{ab}\big((ab)^{(i)}\big) = \mathfrak{ab}\big((ba)^{(i)}\big)$, for all $a, b \in F_S$ and for all $i \in \mathbb{N}$. It is well known (see [1]) that any $\mu \in \mathcal{M}_S^+$ can be written as a power of an indecomposable monomial after cyclic permutations. Thus, by Lemma 2.2.5 one gets that $\mathcal{P}_S^{ab}$ is generated by $\mathfrak{ab}(\mu^{(i)})$, with $i \in \mathbb{N}$ and $\mu \in \mathcal{M}_S^+$.

S. Donkin showed that C_S is the free commutative ring $\bigotimes_{\mu \in \psi} \Lambda_\mu$, where each Λ_μ is a copy of the ring of symmetric functions (see [4],[5]). Then we have a surjection $\theta : C_S \longrightarrow \mathcal{P}_S^{ab}$ given by $e_i(\mu) \mapsto \mathfrak{ab}(\mu^{(i)})$, with $i \in \mathbb{N}$ and $\mu \in \psi$. The result follows since $\pi \cdot \theta = id_{C_S}$. $\square$

We are now ready to prove Theorem 2.2.2

Proof of 2.2.2. The kernel of $\mathcal{P}_S^{ab} \xrightarrow{(\sigma_k)^{ab}} \Gamma_n(F_S)^{ab}$ is generated by the $\mathfrak{ab}\big(f^{(k)}\big)$, with $k > n$ and $f \in F_S^+$. By the previous Lemma and Zubkov Theorem this is exactly the image by θ of the kernel of the projection $C_S \longrightarrow C_S(n)$ and we are done. $\square$

2.3 Let $D_S(n) \subset B_S(n)$ denote the ring of polynomial mappings from the direct sum of $\#S$ copies of $M_n(\mathbb{Z})$ to $M_n(\mathbb{Z})$ that are G-equivariant with respect to the action of simultaneous conjugation on the direct sum of $\#S$ copies of $M_n(\mathbb{Z})$. Then $D_S(n)$ is the ring of covariants of $\#S$ copies of $M_n(\mathbb{Z})$.

Proposition 2.3.1. *Let $\mathbb{Z}\{\zeta_s\} := j_n(F_S)$ be the subring of $B_S(n)$ generated by the generic matrices, then we have the following equality*

$$D_S(n) = C_S(n) \otimes \mathbb{Z}\{\zeta_s\}.$$

Proof. It is clear that $C_S(n) \otimes \mathbb{Z}\{\zeta_s\} \subset D_S(n)$. Let us add one summand to $M_n(\mathbb{Z})^{(S)}$ and set $T := S \cup \{t\}$, with t a symbol. Let $f \in D_S(n)$ and let y be the generic matrix corresponding to the projection of $M_n(\mathbb{Z})^{(T)}$ on the new summand. Consider $e_1(fy) \in C_T(n)$, then one gets

$$e_1(fy) = \sum_{\mu} f_\mu \, e_1(\mu y) = e_1\big((\sum_{\mu} f_\mu \mu) y\big),$$

with $f_\mu \in C_S(n)$, μ a monomial in the generic matrices ζ_s, $s \in S$. By non-degeneracy of the e_1 (=trace) on gets that $f = \sum_\mu f_\mu \mu \in C_S(n) \otimes \mathbb{Z}\{\zeta_s\}$. $\square$

Let us set

$$\eta_n := (\sigma_n)^{ab} \otimes id_{F_S} : \mathcal{P}_S^{ab} \otimes F_S \longrightarrow \Gamma_n(F_S)^{ab} \otimes F_S.$$

For all $f \in \mathcal{P}_S^{ab} \otimes F_S^+$ and $n \in \mathbb{N}$ let

$$\chi_n(f) := f^n + \sum_{i=1}^{n} (-1)^i f^{(i)} f^{n-i} \in \mathcal{P}_S^{ab} \otimes F_S^+$$

be the n-th Cayley-Hamilton polynomial calculated in f.

The following is the main result of this paper.

Theorem 2.3.2. *The following sequence is exact*

$$0 \longrightarrow \langle \{\eta_n(\chi_n(f)) \,:\, f \in \Gamma_n(F_S)^{ab} \otimes F_S^+\} \rangle \longrightarrow \Gamma_n(F_S)^{ab} \otimes F_S \xrightarrow{\pi_n \otimes j_n} D_S(n) \longrightarrow 0.$$

Proof. Let $f \in \mathcal{P}_S^{ab} \otimes F_S$ and let y be a new variable. Then $f \mapsto (fy)^{(1)}$ gives an isomorphism of $\mathbb{Z}$-modules between $ker\big(\mathcal{P}_S^{ab} \otimes F_S \to D_S(n)\big)$ and the sub-$\mathbb{Z}$-module of $ker\big(\mathcal{P}_{S\cup\{y\}}^{ab} \to \Gamma_n(F_{S\cup\{y\}})^{ab}\big)$ of the elements of degree 1 in y. It is then enough to describe the latter.

The ideal $ker\big(\mathcal{P}_{S\cup\{y\}}^{ab} \to \Gamma_n(F_{S\cup\{y\}})^{ab}\big)$ it is generated as a $\mathbb{Z}$-module by elements of the form $gh^{(n+k)}$, with $g \in \mathcal{P}_{S\cup\{y\}}^{ab}$, $h \in \mathcal{P}_{S\cup\{y\}}^{ab} \otimes F_{S\cup\{y\}}^+$ and $k \geq 1$. We claim that its elements of degree 1 in y are of the form $(fy)^{(1)}$, with $f \in \langle \{\chi_{n+k}(a) \,:\, k \in \mathbb{N} \text{ and } a \in \mathcal{P}_S^{ab} \otimes F_S^+\} \rangle$.

Let $d_y(gh^{(n+k)}) = 1$. There are two cases: (1) If $d_y(g) = 1$ then there exists $g^{'} \in \mathcal{P}_S^{ab} \otimes F_S^+$ such that $g = (g^{'}y)^{(1)}$. Then we have

$$gh^{(n+k)} = (g^{'}y)^{(1)}h^{(n+k)} = \big(g^{'}(h\chi_{n+k-1}(h) - \chi_{n+k}(h))y\big)^{(1)}.$$

(2) If $d_y(g) = 0$, then $h = \sum_i h_i$, where $d_y(h_i) = i$ for all $i \in \mathbb{N}$ and $h_1 \neq 0$.

From $h^{(n+k)} = (\sum_i h_i)^{(n+k)} = \sum_{|\alpha|=n+k} \prod_i h_i^{(\alpha_j)}$ one sees that the summand of $h^{(n+k)}$ having degree 1 in y is $h_0^{(n+k-1)}h_1^{(1)}$. Now, for all $k \in \mathbb{N}$ and $a, b \in \mathcal{P}_S^{ab} \otimes F_S^+$ one gets

$$a^{(k)}b^{(1)} = \sum_{i=1}^{k}(-1)^k(a^{k-i}b)^{(1)}a^{(i)} = (\chi_k(a)\, b)^{(1)}.$$

Thus $h_0^{(n+k-1)}h_1^{(1)} = (\chi_{n+k-1}(h_0)h_1)^{(1)}$, and the claim is proved.

To prove the statement it is enough to observe that $ker\eta_n \subset \langle\{\chi_{n+k}(f) : k \in \mathbb{N}\, f \in \mathcal{P}_{\otimes}^{ab} F_S^+\}\rangle$ and that $\chi_{n+k}(f) \equiv f^{n+k}\chi_n(f)(\mod F_S\ ker\eta_n\ F_S)$, for all $h \geq 0$ and for all $f \in \mathcal{P}_S^{ab} \otimes F_S^+$. $\square$

2.4

Definition 2.4.1. *Let R be a ring and let $N : R \longrightarrow R$ be a multiplicative polynomial law homogeneous of degree n, with central values. We call N a homogeneous polynomial norm. Let t be a variable commuting with the elements of R. We set, for all $r \in R$:*

$$\chi_r(t) := N(t - r) = t^n + \sum_{i=1}^{n}(-1)^i N_i(r)t^{n-i}.$$

If $\chi_r(r) = 0$, for all $r \in R$, then we say that (R, N) is a Cayley-Hamilton ring of degree n (with respect to N).

Remark 2.4.2. Let A be a commutative ring. For any integer n, the ring $M_n(A)$ is a Cayley-Hamilton ring of degree n, with respect to the usual determinant.

The ring $D_S(n)$ is a Cayley-Hamilton ring of degree n, with respect to the usual determinant.

The mapping

$$a \mapsto \mathfrak{ab}_n(a^{(n)}), \text{ for all } a \in \Gamma_n(F_S)^{ab} \otimes F_S$$

is a polynomial norm

$$\Gamma_n(F_S)^{ab} \otimes F_S @>>> \Gamma_n(F_S)^{ab}$$

homogeneous of degree n. Notice that $\pi_n\big(\mathfrak{ab}_n(a^{(n)})\big) = det\big(\pi_n \otimes j_n(a)\big)$, for all $a \in \Gamma_n(F_S)^{ab} \otimes F_S$.

Theorem 2.4.3. *For any set S, the ring $D_S(n)$ is free on S in the category of Cayley-Hamilton rings of degree n.*

Proof. Let R be a Cayley -Hamilton ring of degree n with respect to N. Choosen $r_s \in R$ with $s \in S$ there exists a unique ring homomorphism $f : F_S \longrightarrow R$ such that $f(x_s) = r_s$.

Let $Z(R)$ denote the center of R, then $N \cdot f : F_S \to Z(R)$ is a multiplicative polynomial law homogeneous of degree n. Then there is a unique ring homomorphism

$$\phi : \Gamma_n(F_S)^{ab} \to Z(R),$$

such that $\phi \cdot \mathfrak{ab}_n(a^{(n)}) = N \cdot f(a)$, for all $a \in F_S$. The map

$$\phi \otimes f : \Gamma_n(F_S)^{ab} \otimes F_S \to R,$$

is then a ring homomorphism extending f. Obviously this preserves the norm and its kernel must contain

$$\langle \{\eta_n(\chi_n(f)) \,:\, f \in \Gamma_n(F_S)^{ab} \otimes F_S^+\}\rangle,$$

since R is Cayley -Hamilton of degree n. $\square$

§3 The Embedding Problem

3.1 Let $\mathbb{K}$ be an infinite field and let R be a $\mathbb{K}$-algebra, we would like to find sufficient conditions for the existence of a commutative $\mathbb{K}$-algebra, say L, such that R is embeddable into $M_n(L)$. Let us recall the construction of $(A_n(R), j_n^R)$ defined in the Introduction.

Let

$$0 \longrightarrow K \longrightarrow F_S \xrightarrow{\pi} R \longrightarrow 0$$

be any presentation of R by means of generators and relations.

Let J be the two sided ideal of $B_S(n)$ generated by $j(K)$. There exists an ideal I of $A_S(n)$ such that $I = M_n(J)$. Is then easy to show (see [9]) that $A_n(R) = A_S(n)/I$ and that $j_n^R(r) = j_n(f) + M_n(J)$, for all $r \in R$ and $f \in F_S$ such that $\pi(f) = r$.

We showed that any Cayley-Hamilton ring of degree n can be written as a quotient (in the category of Cayley-Hamilton rings of degree n) of a ring of covariants. This result can be regarded as the first step towards a generalization of (the proof of) Procesi's Theorem which would yield a positive answer to the Question.

We would like to describe a possible strategy to achieve such a generalization. For sake of simplicity we put F_S for $\mathbb{K} \otimes F_S$, $A_S(n)$ for $\mathbb{K} \otimes A_S(n)$ and so on.

Lemma 4.1.1. *Let $S' \subset S$ and $I_{S'}$ be the kernel of the natural projection $A_S(n) \longrightarrow A_{S'}(n)$. Let us denote by $J_{S'}$ the kernel of the induced map $D_S(n) \longrightarrow D_{S'}(n)$. It is clear that $J_{S'} = M_n(I_{S'})^G$. The following hold:*

1. *$J_{S'}$ is the smallest ideal of $D_S(n)$, such that $e_i(J_{S'}) \subset J_{S'}$, for all i and containing all the generic matrices ζ_s with $s \notin S'$;*
2. *$\tilde{J}_{S'} := B_S(n) J_{S'} B_S(n)$ is equal to $M_n(I_{S'})$.*

Proof.

(1) Obviously $J_{S'}$ is an ideal of $D_S(n)$ such that $e_i(J_{S'}) \subset J_{S'}$, containing ζ_s with $s \notin S'$. Let $f \in J_{S'}$, we can suppose that $f = g + h$, with g that do not contain any of $\{x'_s : s \in S'\}$, while in each term of h appears at least one between $\{x'_s : s \in S'\}$, as variables or in the form $e_i(MX_j)$ for certain i, with $j \in S'$ and M a monomial ; since one has $0_n = f((M_{s'})_{s' \in S'}, 0, \ldots, 0) = g((M'_s)_{s' \in S'}, (M''_s)_{s'' \in S - S'}) = g((M_s)_{s \in S})$, for all $(M_s)_{s \in S} \in M_n(\mathbb{K})^{(S)}$ it follows that $g = 0$ in $D(n)$. Thus $f = h$ and the assertion follows.

(2) It follows from (1), recalling that $J_{S'} = M_n(I_{S'}) \cap D_S(n)$ and that, by means of the elementary matrices, one can extract the entries of the matrices belonging to $J_{S'}$, thus recovering the generators $\{x_{ij}^s : s \notin S'\}$ of $I_{S'}$ from the matrices $\zeta_s, s \notin S'$. $\square$

Let now $R \cong D_{S'}(n)/J$, with $e_i(J) \subset J$, for all $i = 1, \ldots, n$. If $\{r_s\}_{s \in S'}$ is a set of generators of R , then there exists a set S with $S' \subset S$ and an epimorphism

$$\rho : D_S(n) \longrightarrow D_{S'}(n),$$

such that $\rho(J_{S'}) = J$ (it is enough to send $\{x_s\}_{s\in S'}$ on $\{r_s\}_{s\in S'}$ and x_s, with $s \notin S'$ on the generators of J).

The above epimorphism extends to another

$$\hat{\rho} : A_S(n) \longrightarrow A_{S'}(n)$$

and thus to

$$\tilde{\rho} := M_n(\hat{\rho}) : B_S(n) \longrightarrow B_{S'}(n).$$

Let I be an ideal of $A_{S'}(n)$, such that $\tilde{J} := B_{S'}(n) J B_{S'}(n) = M_n(I)$. Then $A_n(R) = A_{S'}(n)/I$. Notice that $\tilde{\rho}(\tilde{J}_{S'}) = \tilde{J}$.

Since $B_{S'}(n) \cong B_S(n) \bigoplus \tilde{J}_{S'}$ as $GL_n(\mathbb{K})$-modules and $\tilde{\rho}$ restricted to $B_S(n)$ is the identity map, we have that $\tilde{\rho}$ splits and that $\tilde{J}_{S'} \cong Ker(\tilde{\rho})$ by means of $a \longmapsto a - \tilde{\rho}(a)$, where we have identified $\tilde{\rho}$ with $i \circ \tilde{\rho}$, with $i : B_S(n) \hookrightarrow B_{S'}(n)$ the natural embedding.

Let $V := \tilde{J}_{S'} \cap Ker(\tilde{\rho})$ we have the following result. For the definition and the main theorem on good filtrations we refer the reader to [3].

Proposition 4.1.2.

(1) *If* $H^1(GL_n(\mathbb{K}), V) = 0$ *then* $R \hookrightarrow M_n(A_n(R))^{GL_n(\mathbb{K})}$.

(2) *If* $H^1(GL_n(\mathbb{K}), V) = H^2(GL_n(\mathbb{K}), V) = 0$ *then* $R \cong M_n(A_n(R))^{GL_n(\mathbb{K})}$.

(3) *If there is a family* $\{V_t\}_{t\in T}$ *of* G*-submodule of* V*, with* T *a direct set, such that*

i) each V_t *is of countable dimension and has a Good Filtration*

ii) $V = \varinjlim V_t$,

then $R \cong M_n(A_n(R))^{GL_n(\mathbb{K})}$.

Proof.

(1) Use the short exact sequence

$$0 \longrightarrow V \longrightarrow \tilde{J}_{S'} \longrightarrow \tilde{J} \longrightarrow 0$$

and observe that if $H^1(GL_n(\mathbb{K}), V) = 0$ then

$$0 \longrightarrow V^{GL_n(\mathbb{K})} \longrightarrow J_{S'} \longrightarrow \tilde{J}^{GL_n(\mathbb{K})} \longrightarrow 0$$

is exact. But $J_{S'}/V^{GL_n(\mathbb{K})} \cong J \subset \tilde{J}^{GL_n(\mathbb{K})}$ and the statement is proved.

(2) Since $0 = H^1(GL_n(\mathbb{K}), \tilde{J}_{S'}) \cong H^1(GL_n(\mathbb{K}), Ker(\tilde{\rho}))$ the assertion follows from a) using the long cohomology sequence.

(3) If all the V_t s have Good Filtration, then their first cohomology groups are zero. Since H^i commutes with direct limits, it follows that $H^1(GL_n(\mathbb{K}), V) = 0$. Thus we have the embedding.

Under hypotheses that are certainly satisfied here, the quotient of two G-modules having Good Filtrations has Good Filtration too. Hence we can apply to $\tilde{J}$ the observation just done and say that $H^1(GL_n(\mathbb{K}), \tilde{J}) = 0$. Then the surjectivity follows. □

Acknowledgment

I would like to thank C.Procesi for suggesting to work on these topics, for his encouragement and for valuable discussions. I would like also M.Brion for useful remarks on this paper.

This work was done while I was a Senior Fellow at I.N.D.A.M. "Francesco Severi"in Rome - Italy, I would like to thank the President and the staff of this Institute for their support.

References

[1] S.A.Amitsur, *On the Characteristic Polynomial of a Sum of Matrices*, Linear and Multilinear Algebra **8** (1980), 177-182.

[2] P.Berthelot , A.Ogus, *Notes on Crystalline Cohomology*, Princeton University Press, Princeton N.J. (1978).

[3] S.Donkin, *Rational representations of GL: Tensor Products and Filtrations*, LNM 1140, Springer-Verlag (1985).
[4] S.Donkin, *Invariant functions on matrices*, Math. Proc. Camb. Phil. Soc. **113** (1993), 23-43.
[5] S.Donkin, *Invariants of several matrices*, Invent. math **110** (1992), 389-401.
[6] C.Procesi, *The invariant theory of $n \times n$ matrices*, Advan. in Math. **19** (1976), 306-381.
[7] C.Procesi, *Rings with Polynomial Identities*, Lectures Notes in Pure and Appl. Math., Vol.17, Dekker, New York (1973).
[8] C.Procesi, *A Formal Inverse to the Cayley-Hamilton Theorem*, J.Algebra **107** (1987), 63-74.
[9] C.Procesi, *Deformations of Representations*, Preprint (http://mercurio.mat.uniroma1.it/people /procesi/preprints.html).
[10] N.Roby, *Lois polynômes et lois formelles en théorie des modules*, Ann.Ecole Norm. Sup. **80** (1963), 213-348.
[11] N.Roby, *Lois polynômes multiplicatives universelles*, C.R.Acad.SC.Paris **290** (1980), 869-871.
[12] D.Ziplies, *Divided powers and multiplicative polynomial laws*, Comm.Algebra **14** (1986), 49-108.
[13] D.Ziplies, *A Characterization of the Norm of an Azumaya Algebra of Constat Rank through the Divided Powers Algebra of an Algebra*, Beitraege Algebra Geom. **22** (1986), 53-70.
[14] A.N.Zubkov, *Endomorphisms of Tensor Products of Exterior Powers and Procesi Hypothesis*, Comm. Algebra **22** (1994), 6385-6399.
[15] A.N.Zubkov, *On generalization of a theorem of Procesi - Razmyslow*, Algebra and Logic **35, n.4** (1996), 433 - 457 (in Russian).

Dipartimento di Matematica - Politecnico di Torino - Corso Duca degli Abruzzi 24 - 10129 - Torino - Italy e-mail:vaccarino@ syzygie.it